CLAIMS

1.   A computer network intrusion detection system comprising:

an intrusion detector for detecting external attacks upon a computer network;

5   an analyzer coupled to said intrusion detector for analyzing each detected

attack and determining a characteristic indicative thereof; and

a filter coupled to said analyzer for generating an alert based upon

characteristics of a plurality of attacks.

10 2.   The system according to claim 1 wherein said filter generates a first alert

signal in response to an attack having a new characteristic, and further generates a

second alert signal indicative of a predetermined plurality of attacks having the new

characteristic occurring within a predetermined time.

15 3.   The system according to claim 1 wherein said filter generates a first alert

signal in response to an attack having a new characteristic, and further generates a

subsequent first alert signal in response to a subsequent attack having the new

characteristic occurring after an absence of attacks having the new characteristic

occurring within a predetermined time.

20

4.   The system according to claim 1 wherein said filter generates the alert in

response to attacks of a predetermined characteristic exceeding a predetermined

rate or frequency.

5.   The system according to claim 4 wherein the predetermined rate or frequency deterministically varies.

6.   The system according to claim 1 further comprising

5   a second intrusion detector for detecting attacks upon a second computer network, wherein

said filter is further coupled to said second intrusion detector and communicates the alert to the computer network in response to attacks of a predetermined characteristic upon the second computer network exceeding a

10   predetermined rate or frequency.

7.   The system according to claim 1 further comprising:

a vulnerability tester coupled to said analyzer for testing a second computer network for a vulnerability to an attack characteristic detected by said analyzer.

15

8.   The system according to claim 1 further comprising:

an second intrusion detector for detecting external attacks upon a second

computer network;

a second analyzer coupled to said second intrusion detector for analyzing

5   each detected attack upon the second network and determining a characteristic

indicative thereof, wherein

said filter is further coupled to said second analyzer and further compares the

attack characteristics determined by said analyzer and said second analyzer and

generates a general attack alert in response to a substantial similarity in the

10   comparison.

9.   The system according to claim 1 further comprising:

a second intrusion detector for detecting external attacks upon a second

computer network;

15   a second analyzer coupled to said second intrusion detector for analyzing

each detected attack upon the second network and determining a characteristic

indicative thereof, wherein

said filter is further coupled to said second analyzer and further compares the

attack characteristics determined by said analyzer and said second analyzer and

20   generates a specific attack alert in response to a substantial absence of similarity in

the comparison.

10.   The system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks.

5

11.   The system according to claim 9 further comprising:

a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks.

10

12.   A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

determining a characteristic of an attack upon the first network;

determining if the characteristic matches a characteristic of an attack upon a

15   second client coupled to the multiple client network system; and

generating a first alert in response to an absence of the match.

13.   The method according to claim 12 further comprising the step of generating a second alert in response to the presence of the match.

20

14.   The method according to claim 13 wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network.

15. The method according to claim 12 wherein

said step of determining if the characteristic matches a characteristic of an

attack upon a second client determines if the characteristic matches a characteristic

5   of attacks upon multiple clients coupled to the multiple client network system.

16.   A method of preempting an intrusion comprising the steps of:

determining characteristics of an attack upon a first host; and

testing a second host for a susceptibility to an attack of the determined

10   characteristics.

17   The method according to claim 16 further comprising the step of

further determining if the characteristic of the attack upon the first host is a

new characteristic, wherein

15   said step of testing does not test the susceptibility of the second host if said

step of further determining does not determine that the characteristic of the attack

upon the first host corresponds to the new characteristic.

18.   The method according to claim 17 wherein the new characteristic

20   corresponds to a characteristic not previously determined.

19.   The method according to claim 16 further comprising the step of

generating an alert if said step of testing indicates that the second host is

susceptible to the determined characteristics.

5   20.   The method according to claim 16 further comprising the step of

filtering the determined characteristics of a plurality of attacks determined by

said step of determining and generating an alert signal in response to a substantial

increase in frequency or rate of attacks of the characteristic, wherein

said step of testing tests the susceptibility of the second host in response to

10   the alert signal.